

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

OCT 6 2017

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
THE SEARCH OF TARGET DEVICES
DESCRIBED IN ATTACHMENT A
CURRENTLY LOCATED AT 2675
PROSPERITY AVENUE, SUITE 400,
FAIRFAX, VA 20598

Case No. 1:17-SW-670
Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the Northern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section | Offense Description |
|---|--|
| 18 U.S.C. §§ 371, 1028A, 1029, 1030, 1343, 1344, 1349, 1956, 1957 | See attached Affidavit in Support of Search Warrant. |

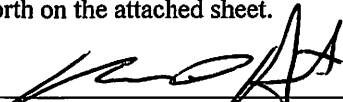
The application is based on these facts:

SEE AFFIDAVIT.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Kellen Dwyer


Applicant's signature


Special Agent Maurice Haughton Homeland Security Investigations
Printed name and title

Sworn to before me and signed in my presence.

Date:

10/6/17

City and state: Alexandria, Virginia

/s/

Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

The Honorable Theresa C. Buchanan, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Property to be Searched

The property to be searched are the following electronic devices (collectively, the “DEVICES”):

1. An Apple iPhone 7 cellular telephone (Model No. MN8G2LL/A; Serial No. F4KSH29QHG6W; bearing IC: 579C-E3085A);
2. An Apple iPhone 6 Plus cellular telephone (Model No. A1522; IMEI No. 354453062299956);
3. An Apple iPhone 5S cellular telephone (Model No. A1533; IMEI No. 013847008746397);
4. An Apple iPhone 6S cellular telephone (Model No. A1688; IC No. 579C-E2946A);
5. An Apple iPhone 6 cellular telephone (Model No. A1549; IC No. 579C-E2816A);
6. An Apple iPhone 6 cellular telephone (Model No. A1549; IMEI No. 354403065170118);
7. A white FedEx Office 32 gigabyte 3.0 USB thumb drive;
8. A purple HP Notebook laptop computer (Model No. 14-AM05ZNR; Serial No. 3CG6482551);
9. A teal Acer laptop computer (Model No. N16W2; Serial No. NXGL2AA001705025316600);
10. A grey Toshiba laptop computer (Model No. Satellite LT5W-B1302; Serial No. E088457S);
11. A DVD diskette with a black and white label; and
12. A skimming device that is a grey colored peripheral strip with red colored trim and white, and blue connectors with some black electrical tape attached.

All of the DEVICES currently are located at HSI Washington Field Office, 2675

Prosperity Avenue, Fairfax, Virginia 201598, which is located within the Eastern District of

Virginia. This warrant authorizes the forensic examination of the DEVICES identified above for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 1028A; access device fraud, in violation of 18 U.S.C. § 1029; computer intrusion, in violation of 18 U.S.C. § 1030; wire fraud, in violation of 18 U.S.C. § 1343; bank fraud, in violation of 18 U.S.C. § 1344; money laundering, in violation of 18 U.S.C. §§ 1956 and 1957; and conspiracy to commit these crimes, in violation of 18 U.S.C. §§ 371, 1349, and 1946, and involve **Timurek K. KHASANOV, Anatoly ZINCHENCKO, Rudolf MEKHAKIAN, Armen SAPLEKCHIAN**, and/or their co-conspirators, since June 2016, including:

- a. documents, communications, or other information relating to the obtaining, purchasing, selling, transmitting, or use of identities or personally identifying information (including names, Social Security numbers, birth dates, payment card numbers, and bank accounts) or financial information associated with individuals other than **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or their co-conspirators;
- b. documents, communications, or other information relating to the obtaining, purchasing, selling, transmitting, or use fake or falsified personally identifying information (including names, Social Security numbers, birth dates, payment card numbers, and bank accounts) or financial information;
- c. documents, communications, or other information relating to the transferring or attempted transferring of money by wire, between bank accounts and/or by or between credit card processing accounts, including the nature, source, destination, and use of those funds;

- d. documents, communications, or other information relating to the purchase, creation, transmission, or use of stolen, falsified, or fake payment card numbers;
- e. documents, communications, or other information relating to the structuring or other concealment of financial transfers and/or withdrawals;
- f. lists or ledgers of payment card numbers issued by financial institutions or credit card companies that to customers of those financial institutions or credit card companies (other than **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or their co-conspirators);
- g. identity documentation, such as visas, passports, driver's licenses, birth certificates, and immigration records;
- h. bank records, checks, credit card bills, account information, and other financial records;
- i. documents, communications, and other information recording **KHASANOV's, ZINCHENCKO's, MEKHAKIAN's**, and/or **SAPLEKCHIAN's** schedule or travel from June 2016 to the present;
- j. communications with co-conspirators regarding the criminal conduct identified above or that would reveal the identity or relationships between co-conspirators;
- k. photographs of co-conspirators involved in the criminal conduct identified above, or that would reveal the identity or relationships between co-conspirators;
- l. documents, communications, and other information regarding the usernames, phone numbers, emails, Skype accounts, or instant messenger names used by **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or

their co-conspirators to transmit information, including personally identifying information, payment card numbers, and false identification documents;

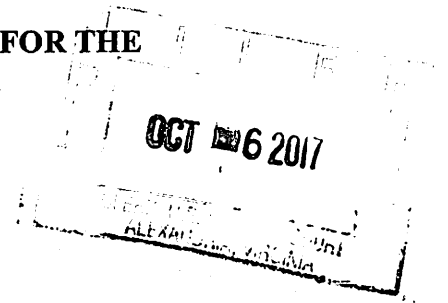
- m. documents, communications, and other information indicating the state of mind as it relates to the crime under investigation of **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or their co-conspirators;

2. Evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division



IN THE MATTER OF THE SEARCH OF
TARGET DEVICES DESCRIBED IN
ATTACHMENT A CURRENTLY LOCATED
AT 2675 PROSPERITY AVENUE, SUITE
400, FAIRFAX, VA 20598

Case No. 1:17-SW-670

Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Maurice Haughton, being duly sworn, depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices, which are described further in the paragraphs below and in Attachment A—that currently is in the possession of federal law enforcement within the Eastern District of Virginia, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”), and have been so employed since April 2009. I currently am assigned to the Financial Investigations Group within HSI’s Washington, D.C. Field Office. I have received training in general law enforcement, including training in Titles 18 and 19 of the U.S. Code, and I am a graduate of the Federal Law Enforcement Training Center at Glynco, Georgia. I have received specialized training in computer crimes, credit card fraud and financial investigations. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States, including:

18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1029 (Access Device Fraud); 18 U.S.C. § 1030 (Computer Fraud); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1344 (Bank Fraud); 18 U.S.C. § 1349 (Wire and Bank Fraud Conspiracy); and 18 U.S.C. §§ 1956 and 1957 (Money Laundering).

3. The facts and information contained in this Affidavit are based on my training and experience, my personal knowledge, my involvement in this investigation, and information that has been provided to me by other law enforcement professionals. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by review of the records, documents, and other physical evidence obtained during the course of this investigation. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. In addition, where conversations or statements are related herein, they are related in substance and in part except where otherwise indicated.

DEVICES TO BE EXAMINED

4. The property to be searched are 12 electronic devise (hereinafter, the “**TARGET DEVICES**”) that currently are located at 2675 Prosperity Avenue, Suite 400, Fairfax, Virginia 20598, which is within the Eastern District of Virginia.

5. The **TARGET DEVICES**, which are further identified in Attachment A, are listed in the chart below along with a brief description of the locations from which they were seized. A more complete description of the circumstances in which the **TARGET DEVICES** were seized is provided in the next section.

| Electronic Device | Place and Date of Seizure |
|---|---|
| Apple iPhone 7 cellular telephone (Model No. MN8G2LL/A; Serial No. F4KSH29QHG6W) | MEKHAKIAN's person incident to his arrest outside the Budget Inn in Falls Church, Virginia on August 8, 2017. |
| Apple iPhone 6 Plus cellular telephone (Model No. A1522; IMEI No. 354453062299956) | Black Lexus driven by ZINCHENKO and KHASANOV at the time of their arrest on August 8, 2017 in Fairfax, Virginia. |
| Apple iPhone 5S cellular telephone (Model No. A1533; IMEI No. 013847008746397) | Black Lexus driven by ZINCHENKO and KHASANOV at the time of their arrest on August 8, 2017 in Fairfax, Virginia. |
| Apple iPhone 6S cellular telephone (Model No. A1688; IC No. 579C-E2946A) | Black Lexus driven by ZINCHENKO and KHASANOV at the time of their arrest on August 8, 2017 in Fairfax, Virginia. |
| Apple iPhone 6 cellular telephone (Model No. A1549; IC No. 579C-E2816A) | Black GMC Yukon driven by MEKHAKIAN and SAPLEKCHIAN at the time of their arrest outside the Budget Inn in Falls Church, Virginia on August 8, 2017. |
| Apple iPhone 6 cellular telephone (Model No. A1549; IMEI No. 354403065170118) | Black GMC Yukon driven by MEKHAKIAN and SAPLEKCHIAN at the time of their arrest outside the Budget Inn in Falls Church, Virginia on August 8, 2017. |
| White Fed Ex Office 32 gigabyte 3.0 USB thumb drive | Room 134 of the Budget Inn in Falls Church, Virginia, on August 8, 2017. |
| Purple HP Notebook laptop computer (Model No. 14-AMO5ZNR; Serial No. 3CG6482551) | Room 134 of the Budget Inn in Falls Church, Virginia, on August 8, 2017 |
| Teal Acer laptop computer (Model No. N16W2; Serial No. NXGL2AA001705025316600) | Room 134 of the Budget Inn in Falls Church, Virginia, on August 8, 2017 |
| Grey Toshiba laptop computer (Model No. Satellite LT5W-B1302; Serial No. E088457S) | Room 134 of the Budget Inn in Falls Church, Virginia, on August 8, 2017 |
| DVD diskette with a black and white label | Room 134 of the Budget Inn in Falls Church, Virginia, on August 8, 2017 |
| A skimming device that is a grey colored peripheral strip with red colored trim and white and blue connectors with some black electrical tape attached. | Room 140 of the Budget Inn in Falls Church, Virginia, on August 8, 2017 |

6. This Affidavit is submitted for the limited purpose of showing probable cause to believe that the **TARGET DEVICES** contain evidence, fruits, contraband, and/or were themselves instrumentalities of the offenses described in Attachment B, particularly aggravated identity theft, in violation of 18 U.S.C. § 1028A; access device fraud, in violation of 18 U.S.C. § 1029; computer intrusion, in violation of 18 U.S.C. § 1030; wire fraud, in violation of 18 U.S.C. § 1343; bank fraud, in violation of 18 U.S.C. § 1344; money laundering, in violation of 18 U.S.C. §§ 1956 and 1957; and conspiracy to commit such offenses, in violation of 18 U.S.C. §§ 371, 1349, and 1956.

7. In addition, the applied-for warrant would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data that also is particularly described in Attachment B.

SUMMARY OF PROBABLE CAUSE

A. Background on the Conspiracy

8. Since in or around June 2016, agents with the HSI and the Fairfax County Police Department (“FCPD”) have been investigated the use of skimming devices to misappropriate payment card numbers, such as credit and debit card numbers, at gas stations in the Eastern District of Virginia and the surrounding areas.

9. The term “skimming devices,” or “skimmers,” refers to computer hardware that can be installed within legitimate electronic payment mechanisms in order to misappropriate payment card information. In my training and experience, criminals frequently target gas pumps because the electronic payment systems attached to these pumps are not as well monitored as systems attached to traditional cash registers. At gas stations, the skimming devices are attached to the electronic components of gas pumps that accept customers’ credit or debit cards and read

those cards in order to render payment for the purchased gasoline.

10. In my training and experience, skimming devices operate as follows. If a customer swipes a payment card through a skimming device, then the skimming device can electronically capture data from the card, such as the payment card number and the personal identification number (“PIN”). This data can be retrieved in a number of ways. If a skimming device is Bluetooth-enabled, then it can transmit the captured data to a Bluetooth-enabled device, such as a laptop or cellular telephone, that is located up to approximately 300 meters away. Conversely, a text-capable skimmer can transmit the captured data via text message to an electronic device capable of receiving text messages. Finally, an SD card-enabled skimmer requires retrieval of the SD Card in order to recover the captured data. Based on this investigation in this case, it appears that the suspects used two types of skimmers: Bluetooth; and SD card.

11. Once payment card numbers are misappropriated via a skimmer, frequently the next step, in my training and experience, is to conduct “cash-outs,” *i.e.*, to use the misappropriated payment cards to conduct fraudulent purchases and ATM withdrawals. In order to conduct cash-outs, criminals typically encode the stolen payment card number onto physical cards. The encoding process typically requires a computer and a magnetic strip reader with rewriting capability, and criminals have been known to re-code calling card, debit card, or credit card magnetic strips with misappropriated payment card numbers. The re-encoded cards are then used to make ATM withdrawals and/or to purchase money orders from the U.S. Post Office. In my training and experience, postal money orders are purchased because they work like cash and generally have higher maximum purchases than one could withdraw from an ATM (*e.g.*, the purchase limit for postal money orders is \$3,000, whereas ATM withdrawal limits are

typically between \$400 and \$600).

12. I also know from my training and experience that when fraudulent purchases or ATM withdrawals are made, the misappropriated payment card data will be sent via a wire communication to servers controlled by the financial institution that issued the misappropriated payment card number. Where a point-of-sale or ATM is located in one state and the financial institution's server is located in another state, then the wire communication typically will cross at least one state line.

13. Based on the above, I believe that the individuals installing skimmers, stealing payment card numbers, and making fraudulent purchases have violated a number of laws, including, aggravated identity theft, in violation of 18 U.S.C. § 1028A; access device fraud, in violation of 18 U.S.C. § 1029; computer intrusion, in violation of 18 U.S.C. § 1030; wire fraud, in violation of 18 U.S.C. § 1343; bank fraud, in violation of 18 U.S.C. § 1344; money laundering, in violation of 18 U.S.C. §§ 1956 and 1957; and conspiracy to commit such offenses, in violation of 18 U.S.C. §§ 371, 1349, and 1956.

B. Summary of Evidence Against Conspirators

14. Based on my investigation to date, I believe that the following individuals have been engaged in a conspiracy to install skimmers in the Eastern District of Virginia and elsewhere, to use them to misappropriate payment card information, and to use that information to make fraudulent purchases and withdrawals: **Timurek K. KHASANOV**; **Rudolf MEKHAKIAN**; **Armen SAPLEKCHIAN**; and **Anatoly ZINCHENCKO**. As demonstrated in subsections C through E below, the **TARGET DEVICES** were seized from vehicles and hotel rooms associated with these individuals and are believed to belong to them.

15. **Armen SAPLEKCHIAN:** I have received from at least one financial institution numerous photographs from ATMs in the northern Virginia area that indicate **SAPLEKCHIAN** is a participant in the aforementioned conspiracy. These photographs are described below.

a. A review of some of these photographs depict an individual who appears to be **SAPLEKCHIAN** conducting ATM withdrawals between on or about July 8, 2017 through on or about August 8, 2017. This individual's face is visible in several of these photographs, and I have compared these photographs with **SAPLEKCHIAN's** booking photograph and confirmed that the photographs appear to depict **SAPLEKCHIAN**.

b. In addition, I have reviewed a photograph provided by a financial institutions depicting a withdrawal on or about July 12, 2017, via a debit card number that had been misappropriated from an Exxon gas station located on Glade Drive in Reston, Virginia, within the Eastern District of Virginia. The photograph depicts that **SAPLEKCHIAN** driving a 2017 Kia Sedona bearing Colorado license plate SQU673. This same vehicle was also observed through BB&T bank surveillance cameras making fraudulent ATM withdrawals at a BB&T ATM located at on Lee Jackson Highway in Chantilly, Virginia. According to records received from AVIS car rental, the Kia was rented from an AVIS located at the Baltimore Washington International Airport from on or about July 10, 2017, to on or about July 12, 2017, by an individual using **SAPLEKCHIAN's** name and a Russian driver's license.

16. **Timurek KHASANOV:** I also have received from several financial institutions numerous photographs from ATMs in the northern Virginia area that indicate **KHASANOV** is a participant in the aforementioned conspiracy. These photographs are described below.

a. A review of some of these photographs depict an individual who appears to be **KHASANOV** conducting ATM withdrawals between on or about May 22, 2017, through

on or about August 8, 2017. This individual's face is visible in several of these photographs, as is a distinctive arm tattoo, and I have compared these photographs with **KHASANOV**'s booking photograph and confirmed that the photographs appear to depict **KHASANOV**.

b. In addition, as described in subsection C below, **KHASANOV** was observed conducting what appeared to be fraudulent ATM transactions and was stopped in possession of cards suspected to have been re-encoded with misappropriated payment card numbers.

17. **Anatoly ZINCENKO:** As described in subsection C below, **ZINCENKO** was stopped in Falls Church Virginia in possession of misappropriated payment card numbers and \$9,800 in postal money orders that were purchased with misappropriated payment card numbers. In addition, as described in subsection E below, law enforcement seized hundreds of cards suspected to have been re-encoded with misappropriated payment card numbers, as well as over \$35,000 in cash and \$49,000 in postal money orders from a hotel room that **ZINCENKO** admitted to staying in.

18. **Rudolph MEKHAKIAN:** I also have received from at least one financial institution numerous photographs from ATMs in the northern Virginia area that indicate **MEKHAKIAN** is a participant in the aforementioned conspiracy. Some of the photographs I have reviewed depict an individual conducting ATM withdrawals between on or about May 19, 2017, through on or about August 8, 2017. The individual's face is visible in several of these photographs, and I have compared these photographs with **MEKHAKIAN**'s booking photograph and confirmed that they appear to depict **MEKHAKIAN**. In addition, as described in subsection D below, **MEKHAKIAN** was caught in possession of five cards that were re-encoded onto physical cards.

C. August 8, 2017 Traffic Stop of a Black Lexus with KHASANOV and ZINCHENKO and Seizure of Their Phones

19. On or about August 8, 2017, I traveled to a BB&T location in Falls Church, Virginia, along with FCPD officers, after receiving reports on suspicious activity at a nearby bank location. At the BB&T, the FCPD officers observed a white male at the outdoor ATM terminal. An FCPD detective who was on scene recognized this person as **KHASANOV** based on several “lookouts” produced by local banks showing **KHASANOV** conducting fraudulent withdrawals from ATMs.

20. The on-scene law enforcement officers observed **KHASANOV** attempt to engage in what appeared to be multiple ATM transactions with what appeared to be multiple payment cards. FCPD Law enforcement officers also observed **KHASANOV** leave the ATM, walk across the street to a parking lot, enter the passenger side of a black 2011 Lexus ES350 bearing Maryland license plate 1A98209, and engage in a brief conversation with the driver of the vehicle. A few minutes later, FCPD officers watched as the Lexus drove out of the parking lot, cross the street, and then park in the Falls Church BB&T parking lot. FCPD officers then observed **KHASANOV** exit the Lexus and approach the same ATM terminal that he was at previously. **KHASANOV** appeared to conduct several more transactions at the ATM, again appearing to utilize multiple payment cards. Based on my training and experience as well as that of the officers on the scene, **KHASANOV**’s behavior was highly consistent with credit card fraud.

21. **KHASANOV** then was observed departing the ATM and re-entering the Lexus, which then drove out of the parking lot and proceeded westbound on East Broad Street / Route 7 toward Arlington Boulevard / Route 50. Law enforcement officers proceeded to follow the

Lexus. As the Lexus, which was traveling in the far left lane, neared the turn for Arlington Boulevard, the vehicle was seen crossing two lanes and then turning right onto Arlington Boulevard. This lane change constituted a traffic violation. As a result, a law enforcement officer with FCPD and the undersigned Affiant then initiated a traffic stop. This stop was justified by Lexus's illegal lane change and by the existence of probable cause to believe that **KHASANOV** and **ZINCHENKO** were engaged in credit or debit card fraud.

22. Law enforcement officers then exited their vehicle and approached the Lexus. In the passenger seat, visible through the windows of the Lexus, there appeared to be multiple gift cards and calling cards. The back of some of these cards were visible, and it appeared someone had written four digit numbers in black ink on the back of these cards. Based on my training and experience, this is highly indicative of credit or debit card fraud for a number of reasons: (1) calling cards and pre-paid gift cards typically do not have PINs so the writing of PINs on the cards indicates that the cards were re-encoded with stolen debit card numbers; and (2) legitimate users of debit card numbers typically do not write the PINs on cards themselves because that defeats the security purpose of the PINs. By contrast, fraudsters typically are unconcerned about security and frequently have too many cards with too many different PINs to remember.

23. Upon approaching the vehicle, an FCPD detective asked the driver, who identified himself as **ZINCHENKO**, to get out of the car. While making this contact, I noticed **KHASANOV**, who was in the passenger seat, opening the vehicle's glovebox and reaching into the glove box. Concerned that he may be reaching for a weapon, I immediately asked **KHASANOV** to get out of the car. During this process, I noticed what appeared to be multiple gift cards within the glovebox, as well as large quantities of cash and what appeared to be money orders from the U.S. Postal Service. Again, in my training and experience, the presence of

multiple gift cards is highly consistent with this fraud scheme, as are postal money orders since, as stated above, they are frequently used to conduct cash-outs of misappropriated payment card numbers.

24. **ZINCHENKO** and **KHASANOV** then were placed under arrest, and an inventory search of the vehicle was conducted by the arresting FCPD detective at the time of arrest according to FCPD General Orders #520.4 policy and procedures. This search revealed several more gift cards within the Lexus, as well as a GPS navigation unit attached to the dashboard that was displaying directions to another BB&T Bank branch in the area. In addition, three of the **TARGET DEVICES** were found during the search of the Lexus: an Apple iPhone 6 Plus cellular telephone (Model No. A1522; IMEI No. 354453062299956); an Apple iPhone 5S cellular telephone (Model No. A1533; IMEI No. 013847008746397); and an Apple iPhone 6S cellular telephone (Model No. A1688; IC No. 579C-E2946A).

25. During a search of **ZINCHENKO's** person that was conducted incident to his arrest, law enforcement recovered approximately \$9,800 in U.S. Postal Service money orders wrapped in toilet paper wrappers, along with a calling card with a four digit number written on it in black ink.

26. All of the gift cards and calling cards recovered during the traffic stop had four digit numbers on their back. In addition, law enforcement officers also ran the physical cards recovered from the traffic stop, including the calling card found on **ZINCHENKO**, through a magnetic strip reader. According to the reader, all of the cards seized during this traffic stop were re-encoded with credit card or debit cards numbers that a financial institution or credit card company had issued to individuals other than **ZINCHENKO** and **KHASANOV**. In addition, the U.S. Postal Inspector Service confirmed that the postal money orders found on

ZINCHENKO's person were purchased with misappropriated payment card numbers.

27. Thereafter, the undersigned Affiant and a Russian interpreter provided **ZINCHENKO** with his *Miranda* advice of rights, and **ZINCHENKO** stated that he understood his rights and wished to speak with law enforcement. During the ensuing interview, **ZINCHENKO** stated that **KHASANOV** had paid for two rooms at an area hotel, that he was staying in room 134, that the room key was in the Lexus, and that he has personal belongings therein.

28. Markedly, during the arrest and processing of **KHASANOV**, I and FCPD law enforcement observed the cellular telephone belonging to **KHASANOV** receive approximately 16 telephone calls. The face of the cellular telephone indicated that the calls were coming from an individual identified merely as "Rudik," which is similar to the first name of **MEHKHAKIAN**.

D. August 8, 2017 Arrest of MEKHAKIAN and SAPLEKCHIAN at the Budget Inn and Seizure of Their Smart Phones

29. On the same day as the vehicle stop discussed above, *i.e.*, on or about August 8, 2017, law enforcement officers travelled to the Budget Inn located on Lee Highway, in Falls Church, Virginia, within the Eastern District of Virginia, based on the information learned through the investigation discussed above. While observing the hotel, law enforcement saw **MEKHAKIAN** and an unidentified male exit a beige Saturn parked in the rear of the hotel parking lot and enter room 140 of the hotel. Law enforcement also noticed that the black GMC Yukon bearing Missouri license plate YK4E4A was parked at the hotel near room 140, which hotel management confirmed had been rented in **KHASANOV's** name since on or about July 31, 2017.

30. While FCPD detectives sought a search warrant for rooms 134 and 140, FCPD uniform officers were charged with watching the rooms and ensuring that members of the conspiracy—including **MEHKHAKIAN**, who, as discussed above, was believed to be constantly calling **KHASANOV**'s phone during **KHASANOV**'s arrest—did not attempt to destroy evidence. Officers were concerned about the Black GMC Yukon described above because of its proximity to room 140 and its out-of-state plates, which was consistent with the conspirators' known use of rental cars. Accordingly, while the Black GMC Yukon was parked in a space near the hotel main office in front, FCPD uniformed officers approached the vehicle and asked the driver for identification. As they approached they noticed crumpled up gift cards sitting on the left thigh of **MEKHAKIAN**, who was in the front passenger seat. The driver then identified himself as **SAPLEKCHIAN** and the rear passengers were identified as **SAPLEKCHIAN**'s spouse and infant child.

31. After the onsite officers called FCPD detectives, it was confirmed that **SAPLEKCHIAN** was on location, based on surveillance photos, as described above, in which he was seen conducting fraudulent withdrawals at ATMs in the Eastern District of Virginia and the surrounding area. At this point, both **MEKHAKIAN** and **SAPLEKCHIAN** were detained and ultimately arrested. While they were detained, they gave consent to search the car. Based on this consent, as well as the existence of probable cause to search and the need to conduct a sweep of the vehicle incident to the stop and arrest, the Black GMC Yukon was seized and later released to **SAPLEKCHIAN**'s spouse.. That search revealed an Apple iPhone 6 cellular telephone (model: A1549, bearing IC: 579C-E2816A, no IMEI number) and an Apple iPhone 6 cellular telephone (model: A1549, bearing IMEI: 354403065170118).

32. Incident to **MEKHAKIAN**'s arrest, FCPD seized an Apple iPhone 7 cellular

telephone (model: MN8G2LL/A; serial number: F4KSH29QH6W; and IMEI number: 359162077387921) along with six physical cards with magnetic strips of which five were determined to have been encoded with payment card numbers not belonging to **MEKHAKIAN**, **SAPLEKCHIAN**, or **KOZLOVA**.

E. Search of Budget Inn Rooms 134 and 140 and Seizure of Computers, DVD, and Skimming Device

33. Pursuant to the search warrant issued by a Fairfax County magistrate judge, law enforcement searched rooms 134 and 140 of the Budget Inn. A number of items were recovered from the rooms, including the ones set forth in the table below:

| Room 134 | Room 140 |
|--|--|
| A black backpack containing three laptops, a payment card reader, a DVD, and a bundle of what appear to be hundreds of payment cards (a sample of these cards were confirmed to contain misappropriated payment card numbers); | A black laptop bag containing a device that based on my experience is believed to be skimming device; |
| A paid in full, bill of sale for a Lexus ES350 AWD (VIN: JTHCE1KS4B0029005) in the name of KHASANOV ; | Tools associated with creating and installing skimming devices connectors |
| Approximately \$35,950 in U.S. currency (approximately \$35,925 of which was found within three pillow cases); | Four red Bluetooth g antennae that, based on my training and experience, are capable of extending the range of skimming devices, such as the one found in the closet of the room in a black laptop bag |
| Approximately \$49,510.45 in money orders; | A plastic bag containing gift card packaging; |
| A Fed Ex Office 32 gigabyte 3.0 USB thumb drive; A purple HP Notebook laptop (model 14-AMO5ZNR; serial number 3CG6482551); A teal Acer laptop (model N16W2; serial | Miscellaneous personal documents in KHASANOV 's name, including a Maryland Department of Correction Identification for KHASANOV . |

| | |
|---|--|
| NXGL2AA001705025316600); A grey Toshiba laptop computer (model Satellite LT5W-B1302; serial E088457S); A DVD diskette with a black and white label | |
|---|--|

All of the items recovered from the two rooms were transported to the FCPD and stored in FCPD's evidence control room.

F. Probable Cause to Search the TARGET DEVICES

34. As summarized above, each of the **TARGET DEVICES** was seized from the person of the above-described conspirators or from a car or hotel room that was being used by a conspirator to facilitate the conspiracy.

35. Based on my training and experience, I know that co-conspirators frequently use phones to communicate information relevant to the conspiracy. Such communications may take the form of text messages, emails, and other forms of electronic communication, which, based on my training and experience, I know can remain on phones for years. This is particularly true for cellular telephones capable of connecting to the internet, or "smart phones," such as the Apple cellular phones listed herein as the **TARGET DEVICES**, which have the capacity to store vast amounts of information and communications for long periods of time. In addition, based on the multiple phone calls that appear to have been made by **MEKHAKIAN** to **ZINCHENKO** at the time of **ZINCHENKO's** arrest, as described in paragraph d above, there is reason to believe that members of the conspiracy were communicating with each other using the **TARGET DEVICES**. Therefore, the phone logs of the **TARGET DEVICES** likely contain information demonstrating, at a minimum, the relationship among the conspirators.

36. Further, based on my training and experience, I know that computers and smart phones, such as the **TARGET DEVICES**, are essential instrumentalities of schemes such as the

one described above. That is so because payment card information is misappropriated electronically and must be electronically transferred to co-conspirators and electronically encoded onto physical cards. This typically involves transferring payment card data via computer or smart phone before the data is then encoded onto physical cards via computer.

37. Based on my training and experience, I also know that conspirators often retain pictures on their smart phones that link them to their co-conspirators and document acts in furtherance of the conspiracy.

38. Based on my training and experience, I also know that smart phones such as the cellular telephones listed herein as the **TARGET DEVICES** often contain information, including GPS information, showing the owner's possible location at various times. I submit that there is probable cause to believe that this information is contained on the **TARGET DEVICES** and would place the conspirators in the vicinity of banks at the time of various fraudulent bank transactions made in furtherance of the conspiracy.

39. Based on my training and experience, I also know that individuals engaged in complex schemes to defraud financial institutions, such as the scheme described above, often keep stores documents, messages, and records related to their schemes on smart phones and computers such as the **TARGET DEVICES**. I submit that there is probable cause to believe that the **TARGET DEVICES** contain such documents, records, and evidence.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

40. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. ***Wireless telephone***: A wireless telephone (or mobile telephone, or cellular telephone, or smart phone) is a handheld wireless device used for voice and data

communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. ***Digital camera:*** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. ***Portable media player:*** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. ***GPS:*** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when THE TARGET DEVICES communicating with each other are in the same state.

41. Based on my training, experience, and research, I know that the Apple iPhones described herein have capabilities that allow them to serve as a wireless telephone, digital camera, PDA, portable media player, GPS navigation device, and computer, and that such devices store data for long periods of time, including contacts lists, text message, emails, location information, internet browsing history, and photographs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

42. I also know from my knowledge, training, and experience that electronic devices, such as the **TARGET DEVICES**, can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

43. ***Electronic Storage.*** There is probable cause to believe that things that were once stored on the **TARGET DEVICES** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

44. ***Forensic evidence.*** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **THE TARGET DEVICES** was used, the purpose of its use, who used it, and when. There is probable

cause to believe that this forensic electronic evidence might be on **THE TARGET DEVICES**

because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). In the case of laptop computers, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device, as here, to obtain payment card numbers without authorization, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

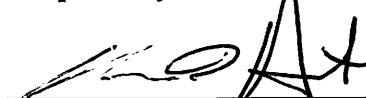
45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

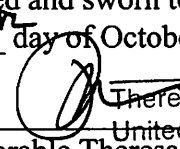
46. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of **THE TARGET DEVICES** described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Maurice Haughton
Special Agent, Homeland Security Investigations

Subscribed and sworn to before me
on this 6th day of October, 2017:

 /s/_____
Theresa Carroll Buchanan
United States Magistrate Judge
The Honorable Theresa C. Buchanan
United States Magistrate Judge

Reviewed by:

Kellen S. Dwyer, Assistant U.S. Attorney, Eastern District of Virginia
Alexander P. Berrang, Assistant U.S. Attorney, Eastern District of Virginia

ATTACHMENT A

Description of Property to be Searched

The property to be searched are the following electronic devices (collectively, the “DEVICES”):

1. An Apple iPhone 7 cellular telephone (Model No. MN8G2LL/A; Serial No. F4KSH29QH6W; bearing IC: 579C-E3085A);
2. An Apple iPhone 6 Plus cellular telephone (Model No. A1522; IMEI No. 354453062299956);
3. An Apple iPhone 5S cellular telephone (Model No. A1533; IMEI No. 013847008746397);
4. An Apple iPhone 6S cellular telephone (Model No. A1688; IC No. 579C-E2946A);
5. An Apple iPhone 6 cellular telephone (Model No. A1549; IC No. 579C-E2816A);
6. An Apple iPhone 6 cellular telephone (Model No. A1549; IMEI No. 354403065170118);
7. A white FedEx Office 32 gigabyte 3.0 USB thumb drive;
8. A purple HP Notebook laptop computer (Model No. 14-AM05ZNR; Serial No. 3CG6482551);
9. A teal Acer laptop computer (Model No. N16W2; Serial No. NXGL2AA001705025316600);
10. A grey Toshiba laptop computer (Model No. Satellite LT5W-B1302; Serial No. E088457S);
11. A DVD diskette with a black and white label; and
12. A skimming device that is a grey colored peripheral strip with red colored trim and white, and blue connectors with some black electrical tape attached.

All of the DEVICES currently are located at HSI Washington Field Office, 2675 Prosperity Avenue, Fairfax, Virginia 201598, which is located within the Eastern District of

Virginia. This warrant authorizes the forensic examination of the DEVICES identified above for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 1028A; access device fraud, in violation of 18 U.S.C. § 1029; computer intrusion, in violation of 18 U.S.C. § 1030; wire fraud, in violation of 18 U.S.C. § 1343; bank fraud, in violation of 18 U.S.C. § 1344; money laundering, in violation of 18 U.S.C. §§ 1956 and 1957; and conspiracy to commit these crimes, in violation of 18 U.S.C. §§ 371, 1349, and 1946, and involve **Timurek K. KHASANOV, Anatoly ZINCHENCKO, Rudolf MEKHAKIAN, Armen SAPLEKCHIAN**, and/or their co-conspirators, since June 2016, including:
 - a. documents, communications, or other information relating to the obtaining, purchasing, selling, transmitting, or use of identities or personally identifying information (including names, Social Security numbers, birth dates, payment card numbers, and bank accounts) or financial information associated with individuals other than **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or their co-conspirators;
 - b. documents, communications, or other information relating to the obtaining, purchasing, selling, transmitting, or use fake or falsified personally identifying information (including names, Social Security numbers, birth dates, payment card numbers, and bank accounts) or financial information;
 - c. documents, communications, or other information relating to the transferring or attempted transferring of money by wire, between bank accounts and/or by or between credit card processing accounts, including the nature, source, destination, and use of those funds;

- d. documents, communications, or other information relating to the purchase, creation, transmission, or use of stolen, falsified, or fake payment card numbers;
- e. documents, communications, or other information relating to the structuring or other concealment of financial transfers and/or withdrawals;
- f. lists or ledgers of payment card numbers issued by financial institutions or credit card companies that to customers of those financial institutions or credit card companies (other than **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or their co-conspirators);
- g. identity documentation, such as visas, passports, driver's licenses, birth certificates, and immigration records;
- h. bank records, checks, credit card bills, account information, and other financial records;
- i. documents, communications, and other information recording **KHASANOV's, ZINCHENCKO's, MEKHAKIAN's**, and/or **SAPLEKCHIAN's** schedule or travel from June 2016 to the present;
- j. communications with co-conspirators regarding the criminal conduct identified above or that would reveal the identity or relationships between co-conspirators;
- k. photographs of co-conspirators involved in the criminal conduct identified above, or that would reveal the identity or relationships between co-conspirators;
- l. documents, communications, and other information regarding the usernames, phone numbers, emails, Skype accounts, or instant messenger names used by **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or

their co-conspirators to transmit information, including personally identifying information, payment card numbers, and false identification documents;

- m. documents, communications, and other information indicating the state of mind as it relates to the crime under investigation of **KHASANOV, ZINCHENCKO, MEKHAKIAN, SAPLEKCHIAN**, and/or their co-conspirators;

2. Evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.